Risk Management Tools

Risk Management Colloquium
Ames Research Center
March 21-22, 2000

Michael A. Greenfield
Deputy Associate Administrator
Office of Safety and Mission Assurance

Outline

- Continuous Risk Management Process
- NASA Risk Management Requirements
- Failure Mode And Effect Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Probabilistic Risk Assessment (PRA)

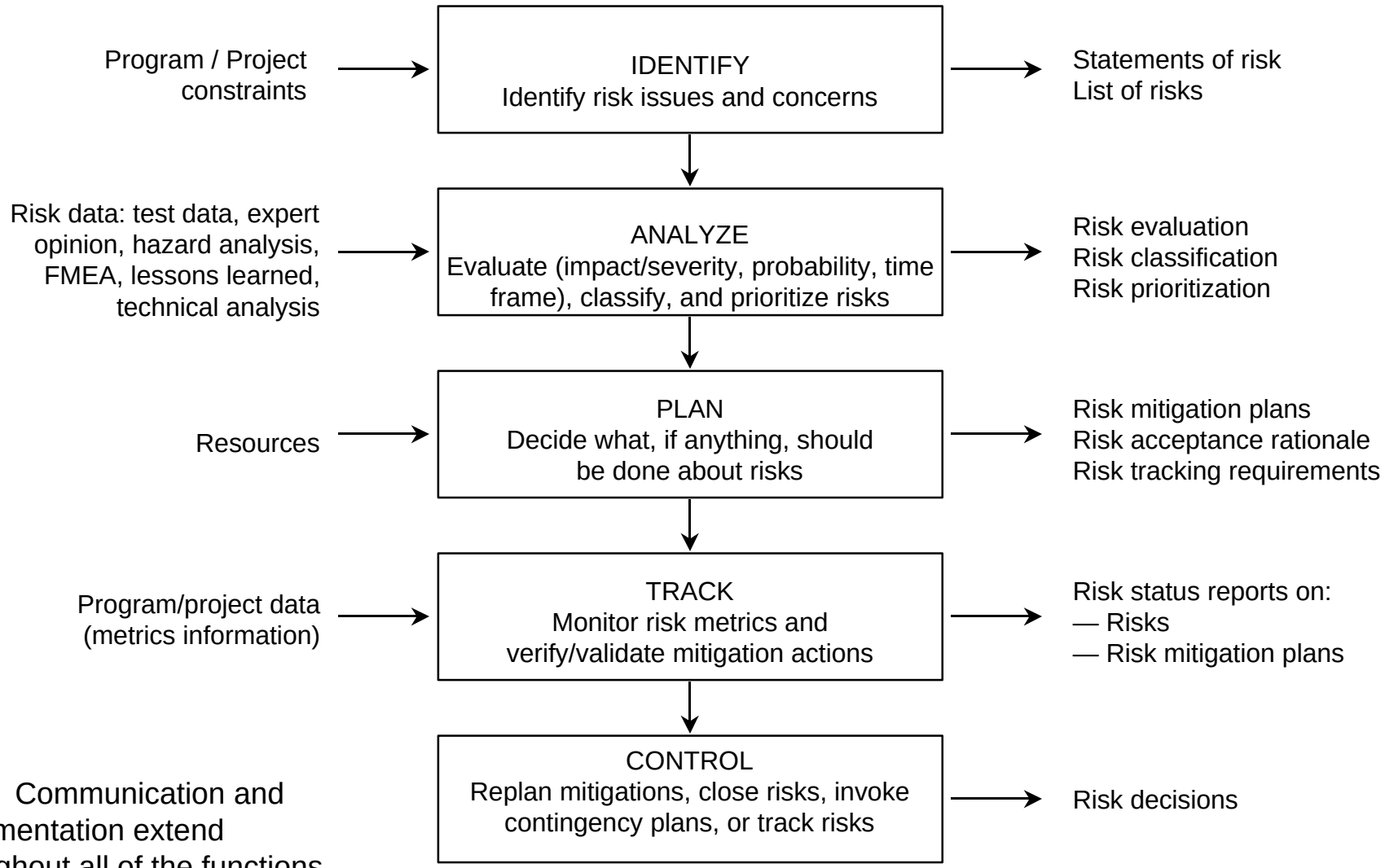
Continuous Risk Management Process

- **Risk management is a continuous process which:**
  - **Identifies risk**
  - **Analyzes risk and its impact, and prioritizes risk**
  - **Develops and implements risk mitigation or acceptance**
  - **Tracks risks and risk mitigation implementation plans**
  - **Assures risk information is communicated to all project/program levels**
- **Risk management planning**
  - **Developed during the program/project formulation phase**
  - **Included in the program/project plans**
  - **Executed/maintained during the implementation phase**
- **Risk management responsibility**
  - **Program/project manager has the overall responsibility for the Implementation of risk management, ensuring an integrated, coherent risk management approach throughout the project**

NASA Risk Management Requirements

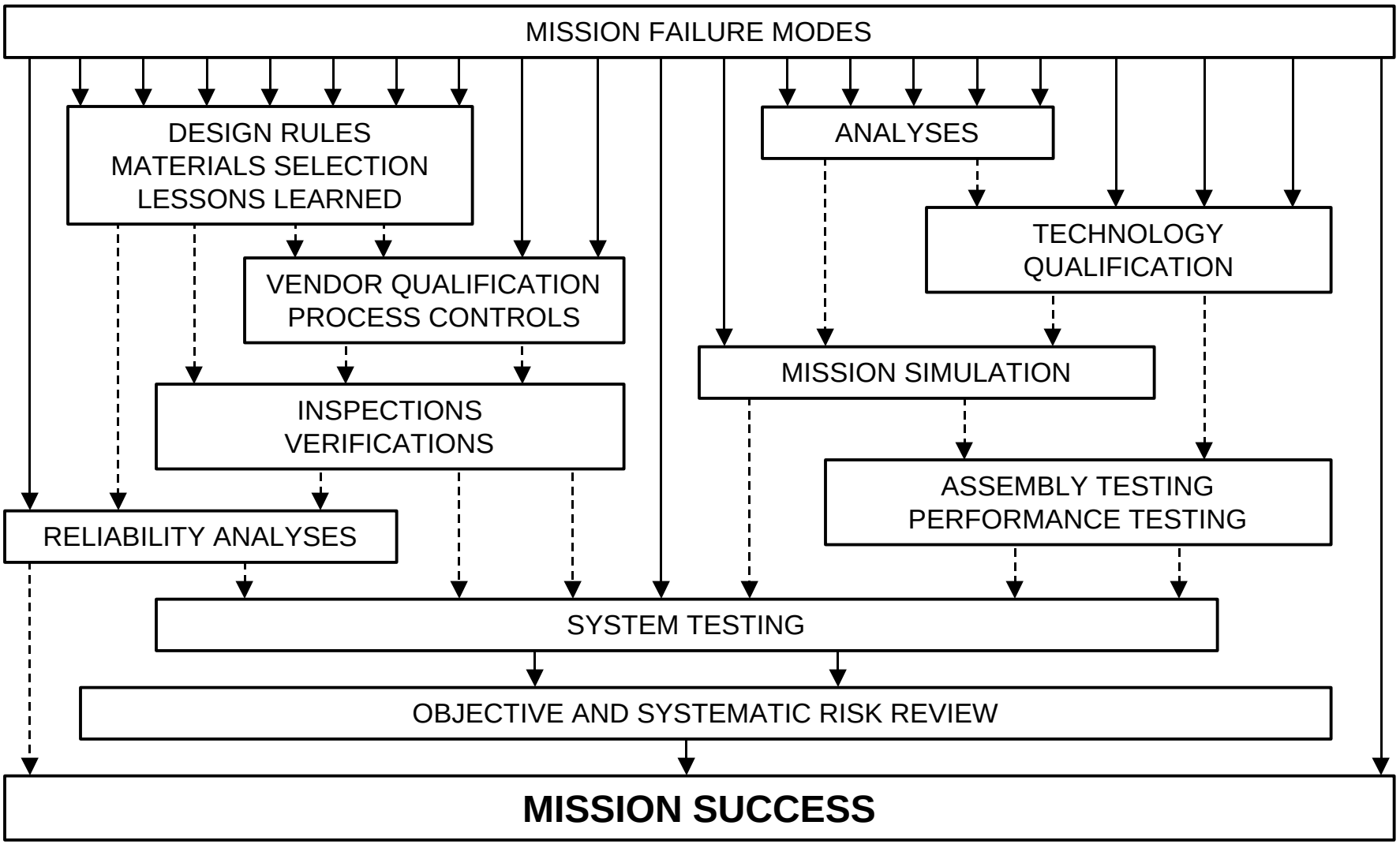
- **NPG 7120.5, NASA Program and Project Management Processes and Requirements**
  - **The program or project manager shall apply risk management principles as a decision-making tool which enables programmatic and technical success**
  - **Program and project decisions shall be made on the basis of an orderly risk management effort**
  - **Risk management includes identification, assessment, mitigation, and disposition of risk throughout the PAPAC (Provide Aerospace Products And Capabilities) process**
- **NPG 8705.x (draft), Risk Management Procedures and Guidelines**
  - **Provides additional information for applying risk management as required by NPG 7120.5**

Risk Management Process



Note: Communication and documentation extend throughout all of the functions.

Mission Success Model



NASA Risk Management Requirements

- **NPG 8715.3, NASA Safety Manual**
  - **Purpose of risk assessment is to identify and evaluate risks to support decision-making regarding actions to ensure safety and mission assurance**
  - **Risk assessment analyses should use the simplest methods that adequately characterize the probability and severity of undesired events**
  - **Qualitative methods that characterize hazards and failure modes and effects should be used first**
  - **Quantitative methods are to be used when qualitative methods do not provide an adequate understanding of failures, consequences, and events**
  - **System safety analysis must include early interaction with project engineering, integration, and operations functions to ensure all hazards are identified**
  - **The hazard assessment process is a principle factor in the understanding and management of technical risk**
  - **As part of the responsibility for overall risk management, the program/project manager must ensure that system safety analyses, appropriate to the program/project complexity, have been conducted**

NASA Risk Management Requirements

- NSTS 22206, instructions for preparation of FMEA and CIL [for Space Shuttle]
  - System and performance requirements are defined
  - Analysis assumptions and groundrules are specified
  - Block diagrams (functional or reliability) are developed
  - Analysis worksheets which include identification of every failure mode are developed (the effects documented address the worst case.)
  - Corrective actions and design improvements are evaluated and recommended
  - Analysis is summarized in report form
- SSP 30234, instructions for preparation of FMEA and CIL [for Space Station]
  - FMEA process, requirements, rules, reporting requirements are described
  - CIL process, requirements, rules, reporting requirements are described
  - Ground support equipment FMEA and CIL processes, requirements, approvals, and databases are described

Failure Mode and Effect Analysis

- FMEA is an inductive engineering technique used at the component level to define, identify, and eliminate known and/or potential failures, problems, and errors from the system, design, process, and/or service before they reach the customer. (Also see MIL-STD-1629)
- FMEA is an early warning or preventative technique that is methodical
  - Systematic method of examining all ways which a failure can occur
  - For each failure, an estimate is made of:
    - Effect on total system
    - Occurrence
    - Severity
    - Detection
  - Bottoms-up analysis based on historical or inferential data at component level
- FMEA will identify corrections required to prevent failures

Failure Mode and Effect Analysis

- **Example**

“For want of a nail, the shoe was lost;
For want of a shoe, the horse was lost;
For want of a horse, the rider was lost;
For want of a rider, the battle was lost;
For want of a battle, the kingdom was lost!”

How would you control the loss of a nail?
Is there more you can do?

A Good FMEA

- Identifies known and potential failure modes
- Identifies causes and effects of each failure mode
- Prioritizes and identifies failure modes according to a Risk Priority Number or similar methods
    - RPN = occurrence x severity x detection
- Provides for problem follow-up and corrective action
- Is updated as product or service develops

FMECA with Reevaluation of Risks

Part Name/ Part Number	Potential Failure Modes	Causes (failure mechanism)	Effects	Risk Priority Rating				Recommended Improvement	Improved Rating			
				Sev*	Freq	Det	RPN		Sev*	Freq	Det	RPN
Pipe	Leakage in pipe	1. Corrosion	Loss of Freon	4	3	8	96	Use stainless steel pipe.	4	1	8	32
		2. Temperature cycling	Loss of Freon	4	3	8	96	Monitor temperature with thermocouples.	4	2	2	16
	Leakage at the joint	1. Cumulative fatigue	Loss of Freon	4	4	8	128	Monitor vibration with acceleration	4	2	2	16
		2. Poor soldering	Loss of Freon	4	4	5	80	Update process FMEA	TBD	TBD	TBD	TBD
Valve	Sticky, intermittent	1. Dirt or foreign objects	Loss of control of temperature	7	3	8	168	Electronic redundant valve action and fault identification	7	1	1	7
	Stuck open	1. Component wearout	Loss of control of temperature	7	2	8	112	Electronic redundant valve action and fault identification	7	1	1	7
	Stuck closed	1. Component failed	Loss of control of temperature	9	2	8	144	Electronic redundant valve action and fault identification	7	1	1	7
		2. Component expansion and contraction	Loss of control of temperature	9	2	8	144	Electronic redundant valve action and fault identification	7	1	1	7

*Severity ratings 8 to 10 request special effort in design improvement regardless of RPN rating

Other Uses for FMEA

- Reliability prediction
- Sub FMEA's
  - System FMEA - components, subsystems, main system
  - Design FMEA - components, subsystems, main system
  - Process FMEA - manpower, machine, method, material, measurement, environment
  - Service FMEA - manpower/human resources, machine, method, material, measurement, environment
- Early integration of quality and manufacturing
- Analysis for:
  - Safety
  - Maintainability
  - Logistics support
  - Mechanic training
- Software; identifies missing requirements, identifies sneak paths in codes
- Reliability; identifies critical paths that may need testing
- FMEA is limited when multiple failure modes occur at the same time

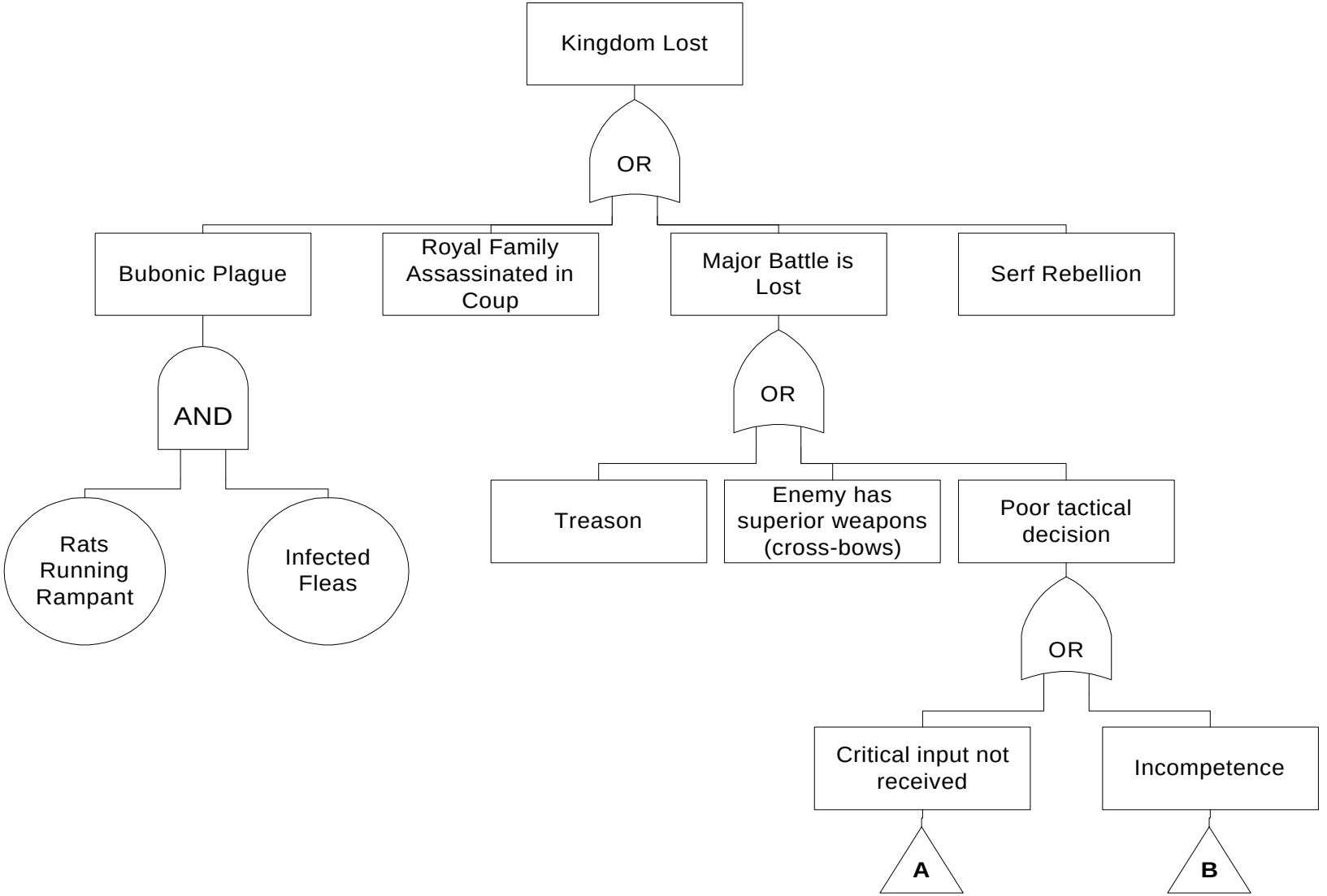
Fault Tree Analysis

- **Background**
  - **FTA is a deductive analytical technique of reliability and safety analyses and generally is used for complex dynamic systems**
  - **FTA provides an objective basis for analysis and justification for changes and additions**
  - **First developed by Bell Telephone in 1961 then modified by Boeing for wide uses**

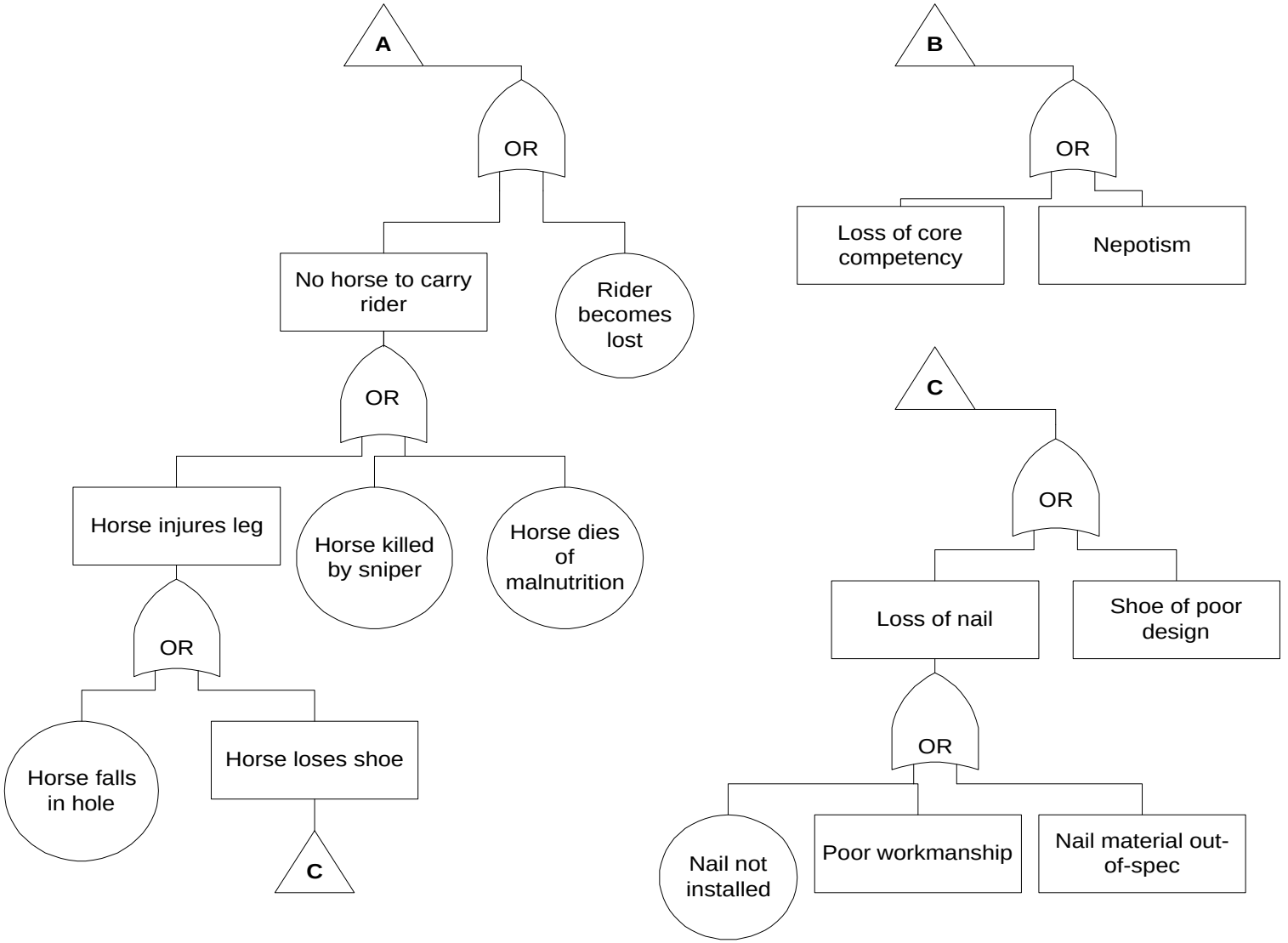
Fault Tree Analysis

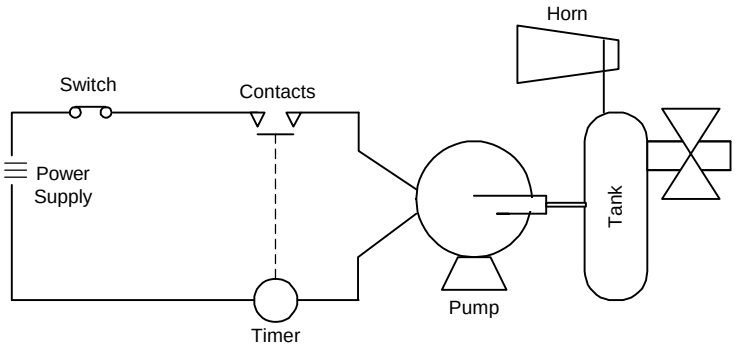
- **Concept**
  - **A model that logically and graphically represents the various combinations of possible events, both faulty and normal, occurring in a system that leads to the top undesired event, e.g., electrical fire in motor circuit**
  - **FTA uses a tree to show the cause-and-effect relationships between a single, undesired event (failure) and the various contributing causes**
  - **The tree shows the logical branches from a single failure at the top of the tree to the root cause(s) at the bottom of the tree**
  - **Standard logic symbols connect the branches of the tree. For example, "gates" permit or inhibit the passage of fault logic up the tree through the "events."**
  - **Fault tree does not necessarily contain all possible failure modes of the components of the system. Fault tree contains only those failure modes whose existence contribute to the existence of the top event.**

Fault Tree


Kingdom Lost
OR
Bubonic Plague
Royal Family Assassinated in Coup
Major Battle is Lost
Serf Rebellion
AND
OR
Rats Running Rampant
Infected Fleas
Treason
Enemy has superior weapons (cross-bows)
Poor tactical decision
OR
Critical input not received
Incompetence
A
B

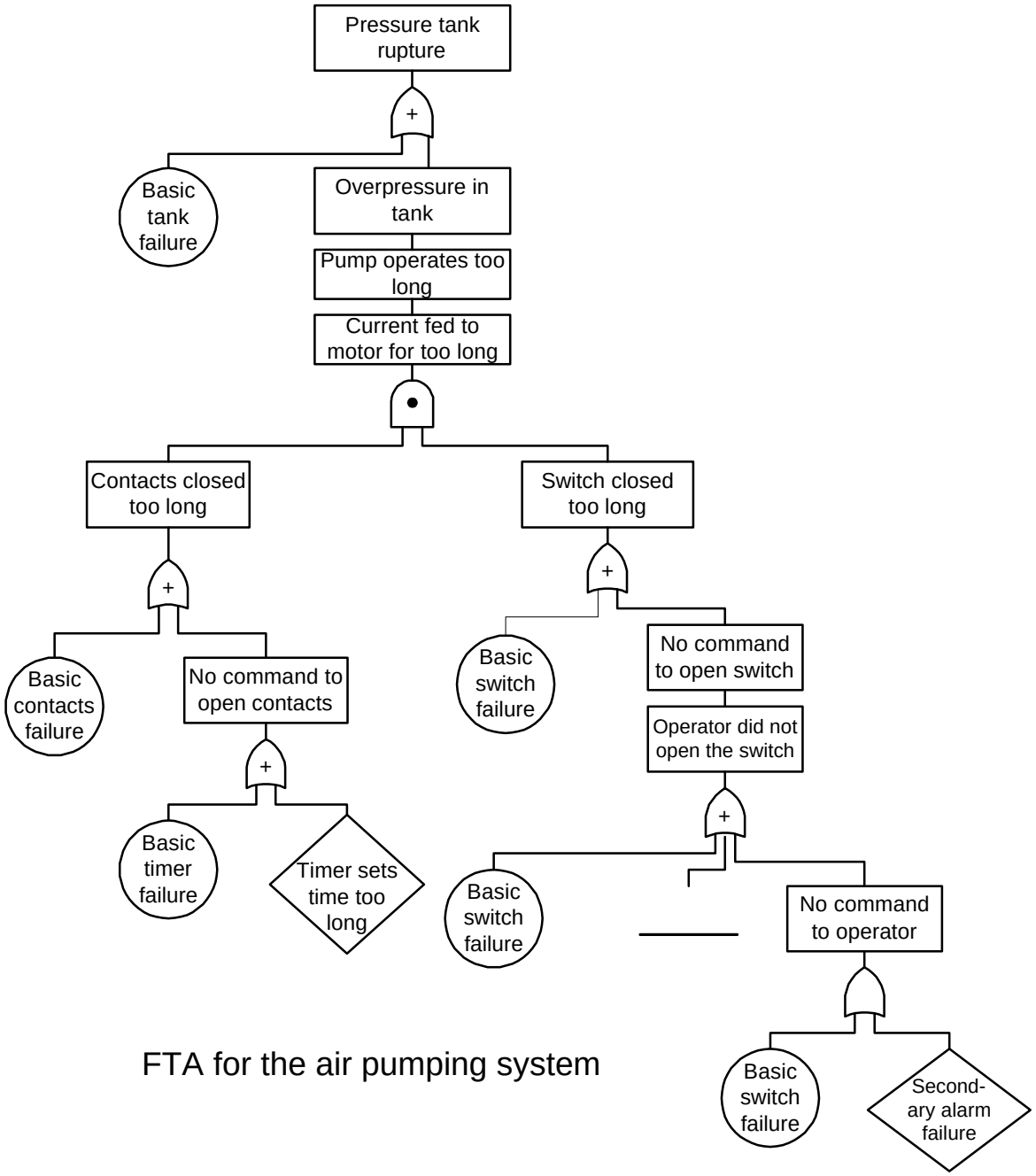
Fault Tree -- Additional Branches





A typical air pumping system

Example 11 - FTA development of an air pumping system



FTA for the air pumping system

Fault Tree Analysis

- **Uses**
  - **Provides the analyst with insight into system behavior**
  - **Allows the analyst to concentrate on one particular system failure at a time**
  - **Identifies ways that failure of a product can lead to an accident**
  - **FTA supplements failure mode and effect analysis**
  - **Helps identify the reliability of higher-level assemblies or the system**
  - **Supports study of the probability of occurrence for each of the root causes**
  - **Assesses the impact of design changes and alternatives**
  - **System analysis via hardware fault tree may be linked to software fault tree**
  - **Isolates critical safety failures**
  - **Provides documented evidence of compliance with safety requirements**
  - **Provides options for qualitative, as well as quantitative, system reliability analysis**

Probabilistic Risk Assessment

- **What is PRA?**
  - **It is an analysis of the probability (or likelihood) of occurrence of a consequence of interest, and the severity of that consequence, including assessment and display of uncertainties**
  - **It is an engineering process, based on comprehensive systems analysis with analytical support, repeated periodically as the design matures and new data become available**
  - **It is a means to express quantitatively *our state of knowledge* about the risk of failure**
  - **It does not guess failure rates, or otherwise create data**

Probabilistic Risk Assessment

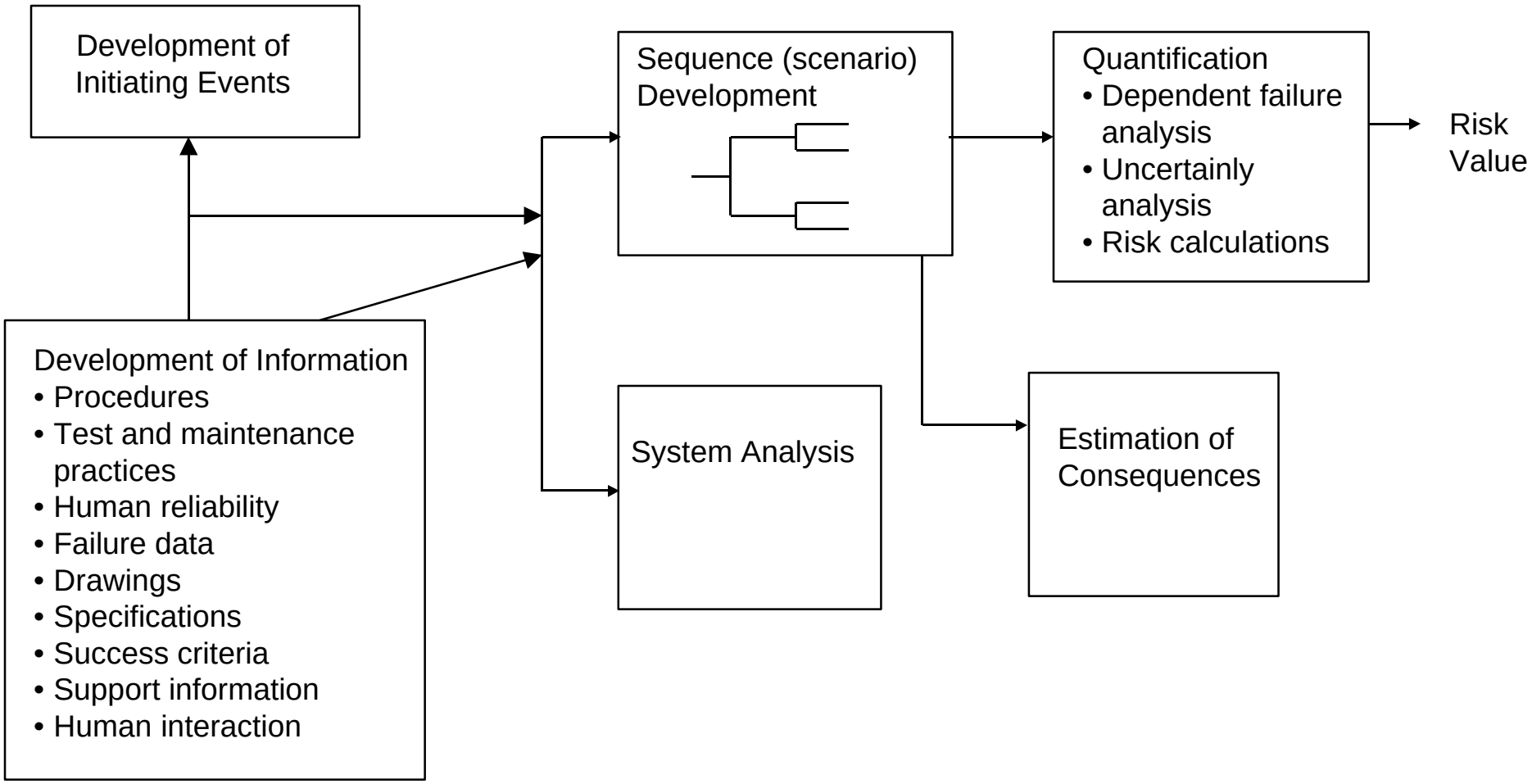
→ **What is PRA used for in NASA programs?**

- For strategic decision support; e.g., What is the probability of successfully assembling the multi-billion dollar International Space Station?
- For systems under development, to guide trade-offs between safety, reliability, cost, performance, and other tradable resources
- For mature systems, to support decision-making on risk acceptability, and (when risk is considered to be too high) on choices among options for risk reduction; e.g., Space Shuttle upgrades
- To track risk levels:
  - Throughout the life cycle
  - To measure effectiveness of risk reduction options

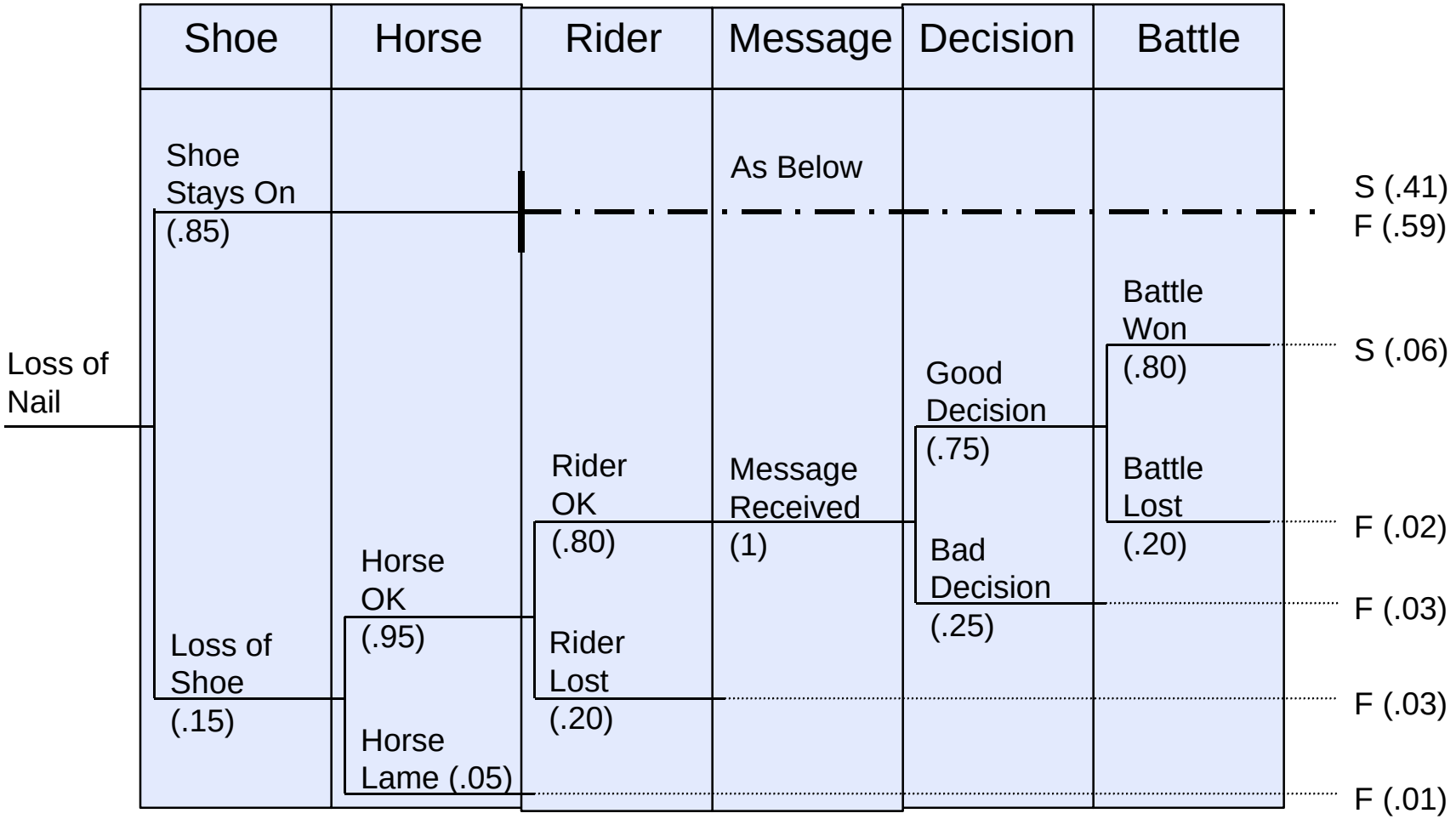
Probabilistic Risk Assessment

- **Methodology**
  - **Step 1: Identification of end states of interest**
  - **Step 2: System familiarization**
  - **Step 3: High-level logic modeling to identify initiating events**
  - **Step 4: Mid-level logic modeling to identify scenarios that can lead from initiating events to end states of interest (e.g., event trees)**
  - **Step 5: Low-level data gathering and modeling to quantify initiating and pivotal events in scenarios (e.g., fault tree)**
  - **Step 6: Aggregation of risk for like end states to produce baseline results (e.g., Monte Carlo)**
  - **Step 7: Sensitivity/importance analysis to identify areas for risk reduction**

Process of Probabilistic Risk Analysis



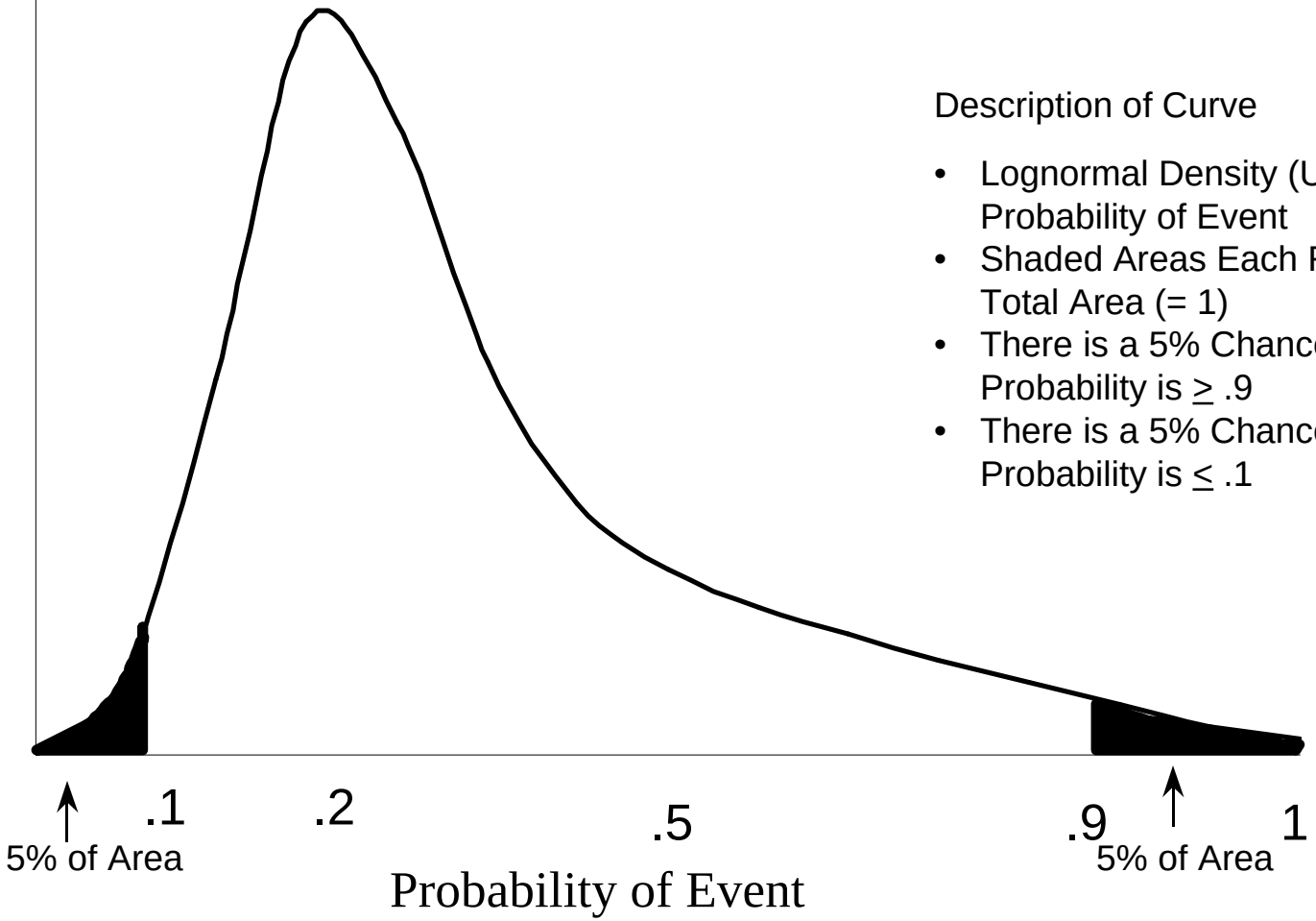
Event Sequence Diagram



41% chance of success (normalized)

Uncertainty Distribution (Log Normal)

Mean is .2; 5% and 95% Percentile Are .1 And .9

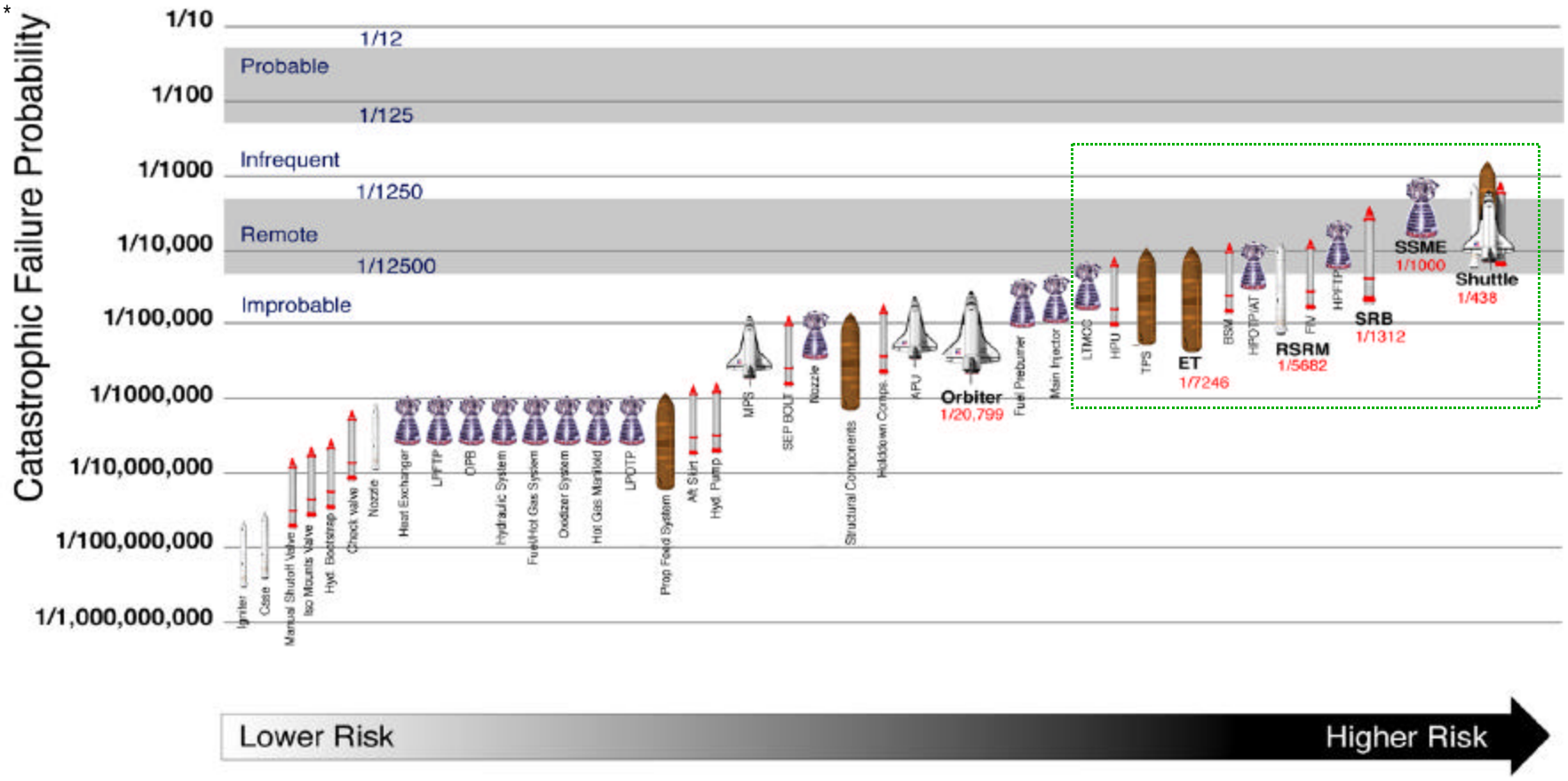


Description of Curve

- Lognormal Density (Uncertainty) on Probability of Event
- Shaded Areas Each Represent 5% of Total Area (= 1)
- There is a 5% Chance that the True Probability is ≥ .9
- There is a 5% Chance that the True Probability is ≤ .1

Space Shuttle Program Development Office

Block IIA Configuration - Ascent



* Based on 1998 QRAS

Space Shuttle Program Development Office

Reliability Sensitivities Analysis - Space Shuttle Ascent

Shuttle Element	Current Reliability **		What ifs ?			
			Element Risk is Cut in 1/2		Element Reliability is Perfect	
	Element	Shuttle	Element	Shuttle	Shuttle	
SSME	1.0x10-03* 1/1000		5.0x10-4 1/2000	1/560		1/779
SRB	7.6x10-04 1/1312		3.8x10-4 1/2624	1/525		1/657
RSRM	1.8x10-04 1/5682	1/438	8.8x10-5 1/11,364	1/455		1/474
ET	1.4x10-04 1/7246		6.5x10-5 1/4,492	1/451		1/466
Orbiter	4.8x10-05 1/20,619		2.4x10-5 1/41,238	1/441		1/447

* Based on SSME Block IIA Configuration

** Based on 1998 QRAS

Probabilistic Risk Assessment

- **Other Advantages of PRA**
  - Component failure distributions are not constant over time
  - System or process may be highly complex
  - Failure may vary with sequence of operation
  - Network logic and paths may not be fully understood for the desired repeatable outcome
  - System or process may be tightly coupled
  - Better definition of fault diagnosis procedures
  - System or process may be very short in duration
  - Testing may not be an option before full-up operation
  - Sensitivity characteristics of the system or process are needed

Summary

- → Continuous Risk Management is not only a requirement but makes good engineering sense
- → Project management is risk management!
- → The application of risk management processes and tools such as FMEA, FTA, and PRA provide a disciplined approach to uncover inherent risks
- → The real payoff occurs during the formulation phase where risk mitigation is generally more effective and cheaper
- → The application of tools is not without cost but the positive ROI from future cost avoidance is well documented

References

- Stamatis, D. H. 1995. *Failure Mode and Effects Analysis.* Milwaukee, WI: Quality Press (permission for certain reproduction being sought.)
- Raheja, Dev G. 1991. *Assurance Technologies Principles and Practices.* USA: McGraw-Hill, Inc. (permission for certain reproduction being sought.)
- National Aeronautics and Space Administration, NSTS 22206, *Instructions for Preparation of Failure Modes and Effects Analyses and Critical Items List,* Houston, TX, NSTS Program Office, Johnson Space Center.
- Henley, J.H. and Kumamoto, H. 1992. *Probabilistic Risk Assessment.* New York, NY: IEEE Press (permission for certain reproduction being sought.)